UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/762,653	01/21/2004	Hidema Tanaka	43521-1600	5291

21611 7590 07/19/2007

SNELL & WILMER LLP (OC)
600 ANTON BOULEVARD
SUITE 1400
COSTA MESA, CA 92626

EXAMINER
TRAN, ELLEN C

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
07/19/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/762,653	**Applicant(s)** TANAKA ET AL.	
	Examiner Ellen C. Tran	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 January 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Ellen Tran

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *APR'04*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is responsive to: an original application filed on 21 January 2004.

2. Claims 1-10 are pending; claims 1-10, are independent claims.

3. The IDS submitted 18 April 2004 has been considered.

Claim Objections

4. Claims 1-10, are objected to because of the following informalities: the claims all indicate "parameter A" this is confusing to the meaning of the claims because "A" could be interpreted as a word. Appropriate correction is required. It is recommended a comma (",") be placed after all of the "parameter A"s or the letter A be changed.

5. Claims 4, is objected to because of the following informalities: the 'an' before predetermined-step estimated' (claims page 35, line 10) should be an 'a'. Appropriate correction is required.

Claim Rejections - 35 USC § 103

6 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7 **Claims 1-10,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith et al. U.S. Patent No. 6,189,095 (hereinafter '095) in view of Ohkuma et al. U.S. Patent No. 7,227,948 (hereinafter '948).

As to independent claim 1, "A cipher strength evaluation apparatus for evaluating strength on ciphertext outputted by a Feistel encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key, and calculating stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:" is taught in '095 col. 5, lines 41-67, note providing a user choices of strength of the cipher is equivalent 'A cipher strength evaluation apparatus';

"an estimated plaintext calculating part for accepting predetermined-step stirred text being stirred text at a predetermined step, calculating an estimated parameter A estimated as a parameter A determined from a predetermined-step extended key being an extended key at a predetermined step, and calculating estimated plaintext based on the predetermined-step stirred text and the estimated parameter A" is shown in '095 col. 6, lines 1-7;

"an encryption control part for using and allowing an encryption apparatus to calculate estimated ciphertext based on the estimated plaintext calculated by the estimated plaintext calculating part" is disclosed in '095 col. 6, line 64 through col. 7, line 10;

"a key verification part for formulating an encryption equation with higher order differences based on the predetermined-step stirred text accepted by the estimated plaintext calculating part and the estimated ciphertext calculated under the control of the encryption control part" is taught in '095 col. 10, lines 39-67;

"processing it by an algebraic technique to try to calculate a last-step estimated extended key estimated as an extended key at a last step" is shown in '095 col. 11, lines 1-25; the following is not explicitly taught in '095:

"verifying the parameter A to be right by detecting that the last-step estimated extended key can be calculated, calculating a right last-step estimated extended key with a predetermined probability, and outputting a calculation impossible signal when detecting that calculation is impossible" however '948 teaches the maximum differential probability is an important measure for estimating the strength of a given function in col. 5, lines 32-60;

"and a decryption control part for accepting the calculation impossible signal, and controlling the estimated plaintext calculating part, the encryption control part, and the key verification part to allow the last-step estimated extended key to be calculated" however '948 teaches decryption has a structure obtained by reversing the encryption apparatus (the same key is used) in col. 17, lines 27-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention a symmetric block cipher using multiples stages with modified type-I and type-3 Feistel networks taught in '095 to include a means to calculate the probability of the last-step extended key. One of ordinary skill in the art would have been motivated to perform such a modification because the typical Feistel type encryption scheme need to improve strength analysis see '948 (col. 1, lines 21 et seq,) "Typical fundamental structures of common key block encryption scheme include SPN type and Feistel type. For both structures, a design method for improving strength evaluation and resiliency against differential/linear cryptanalysis have been studied (reference [1] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers & E. Dcwin, "The Cipher

SHARK," Fast Software Encryption, LNCS 1039, 1996, reference [2] Kazumaro Aoki, Kazuo Ota, "More Strict Evaluation of Maximum Mean Differential Probability and Maximum Mean Linear Probability," SCIS 96-4A, 1996, reference [3], Mitsuru Matsui, "Block encryption scheme MISTY," ISEC 96-11, 1996)".

As to independent claim 2, this claim incorporates similar limitations as independent claim 1, and is also taught by '095 and '948. Below are the limitations that are different from claim 1:

"a second predetermined-step estimated stirred text calculating part for accepting the estimated ciphertext calculated under the control of the encryption control part, calculating a last-step estimated extended key estimated as an extended key at the last step, and calculating second predetermined-step estimated stirred text estimated as stirred text at a second predetermined step based on the estimated ciphertext and the last-step estimated extended key" is taught in 'col. 5, lines 40-67 and col. 6, lines 7-24;

"a key verification part for formulating an encryption equation with higher order differences based on the predetermined-step stirred text accepted by the estimated plaintext calculating part and the second predetermined-step estimated stirred text calculated by the second predetermined-step estimated stirred text calculating part" is taught in '095 col. 10, lines 39-67;

"processing it by an algebraic technique to try to calculate a second predetermined-step estimated extended key estimated as an extended key at the second predetermined step" is shown in '095 col. 11, lines 1-25;

the following is not explicitly taught in '095:

“verifying the parameter A and the last-step estimated extended key to be right by detecting that the second predetermined-step estimated extended key can be calculated, and outputting a calculation impossible signal when detecting that calculation is impossible” however ‘948 teaches the maximum differential probability is an important measure for estimating the strength of a given function in col. 5, lines 32-60;

“and a decryption control part for accepting the calculation impossible signal, and controlling the estimated plaintext calculating part, the encryption control part, the second predetermined-step estimated stirred text calculating part, and the key verification part to allow the second predetermined-step estimated extended key to be calculated” however ‘948 teaches decryption has a structure obtained by reversing the encryption apparatus (the same key is used) in col. 17, lines 27-67.

As to independent claim 3, this claim incorporates similar limitations as independent claims 1, and is also taught by ‘095 and ‘948. Note “a first-step” is considered equivalent to ‘a predetermined step’.

Below are the limitations that are different from claim 1: **“an extended key at the first step by exhaustive search”** is taught in ‘095 in col. 6, lines 8-24.

As to independent claim 4, this claim incorporates similar limitations as independent claims 1-3, and is also taught by ‘095 and ‘948. Note “a first-step” is considered equivalent to ‘a predetermined step’. In addition **‘an predetermined-step estimated stirred text calculating’** is interpreted to be equivalent to ‘a second predetermined-step estimated stirred text’ claim in claim 2.

As to independent claim 5, this claim incorporates similar limitations as independent claims 1-4, and is also taught by '095 and '948. Note "a first-step" is considered equivalent to 'a predetermined step'. In addition **'a last-but-one-step estimated stirred text calculating'** is interpreted to be equivalent to 'a second predetermined-step estimated stirred text' claim in claim 2.

As to independent claim 6, this claim incorporates similar limitations as independent claims 1-5, and is also taught by '095 and '948. Below are the limitations that are different from claim 1-5:

"an estimated stirred text calculating part for accepting the plaintext satisfying a predetermined condition" is shown in '095 col. 6, lines 1-40;

"and calculating predetermined-step estimated stirred text satisfying a predetermined condition and estimated as stirred text at a predetermined step based on the plaintext and the estimated parameter A" is taught in '095 col. 6, lines 7-25;

"a key verification part for formulating an encryption equation with higher order differences based on the predetermined-step estimated stirred text calculated by the estimated stirred text calculating part and the ciphertext calculated under the control of the encryption control part" is disclosed in '095 col. 6, line 64 through col. 7, line 10;

As to independent claims 7 and 8, these claims incorporate similar limitations as independent claims 1-6, and are also taught by '095 and '948.

As to independent claim 9, "A cipher strength evaluation apparatus for evaluating strength on ciphertext outputted by a Feistel encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key, and calculating stirred text

for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:" is taught in '095 col. 5, lines 41-67, note providing a user choices of strength of the cipher is equivalent 'A cipher strength evaluation apparatus';

"an estimated stirred text calculating part for accepting the plaintext satisfying a predetermined condition, calculating an estimated parameter A estimated as a parameter A determined from a first-step extended key being an extended key at a first step by exhaustive search, and calculating first-step estimated stirred text satisfying a predetermined condition and estimated as stirred text at a first step based on the plaintext and the estimated parameter A" is shown in '095 col. 6, lines 1-24;

"an encryption control part for using and allowing an encryption apparatus to calculate ciphertext based on the plaintext accepted by the estimated stirred text calculating part" is disclosed in '095 col. 6, line 64 through col. 7, line 10;

"a predetermined-step estimated stirred text calculating part for accepting the ciphertext calculated under the control of the encryption control part, calculating a last-step estimated extended key estimated as an extended key at a last step, and calculating predetermined-step estimated stirred text estimated as stirred text at a predetermined step based on the ciphertext and the last-step estimated extended key" is taught in '095 col. 5, lines 40-67;

"a key verification part for formulating an encryption equation with higher order differences based on the first-step estimated stirred text calculated by the estimated stirred text calculating part and the predetermined-step estimated stirred text calculated by the

predetermined-step estimated stirred text calculating part" is taught in '095 col. 10, lines 39-67;

"processing it by an algebraic technique to try to calculate a predetermined-step estimated extended key estimated as an extended key at the predetermined step" is shown in '095 col. 11, lines 1-25;

the following is not explicitly taught in '095:

"verifying the parameter A and the last-step estimated extended key to be right by detecting that the predetermined-step estimated extended key can be calculated, and outputting a calculation impossible signal when detecting that calculation is impossible" however '948 teaches the maximum differential probability is an important measure for estimating the strength of a given function in col. 5, lines 32-60;

"and a decryption control part for accepting the calculation impossible signal, and controlling the estimated stirred text calculating part, the encryption control part, the predetermined-step estimated stirred text calculating part, and the key verification part to allow the predetermined-step estimated extended key to be calculated" however '948 teaches decryption has a structure obtained by reversing the encryption apparatus (the same key is used) in col. 17, lines 27-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention a symmetric block cipher using multiples stages with modified type-I and type-3 Feistel networks taught in '095 to include a means to calculate the probability of the last-step extended key. One of ordinary skill in the art would have been motivated to perform such a modification because the typical Feistel type encryption scheme need to improve strength analysis see '948 (col. 1, lines 21 et seq,) "Typical fundamental structures of common key block encryption scheme include SPN type and Feistel type. For both structures, a design method for improving strength evaluation and resiliency against differential/linear cryptanalysis have been studied (reference [1] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers & E. Dcwin, "The Cipher SHARK," Fast Software Encryption, LNCS 1039, 1996, reference [2] Kazumaro Aoki, Kazuo Ota, "More Strict Evaluation of Maximum Mean Differential Probability and Maximum Mean Linear Probability," SCIS 96-4A, 1996, reference [3], Mitsuru Matsui, "Block encryption scheme MISTY," ISEC 96-11, 1996)".

As to independent claim 10, "A cipher strength evaluation apparatus for evaluating strength on ciphertext outputted by a Feistel encryption apparatus having a plurality of steps of accepting unstirred text, stirring with an extended key, and calculating stirred text for encrypting plaintext step by step, the cipher strength evaluation apparatus comprising:" is taught in '095 col. 5, lines 41-67, note providing a user choices of strength of the cipher is equivalent 'A cipher strength evaluation apparatus';

"an estimated stirred text calculating part for accepting the plaintext satisfying a predetermined condition, calculating an estimated parameter A estimated as a parameter A determined from a first-step extended key being an extended key at a first step by exhaustive search, and calculating first-step estimated stirred text satisfying a predetermined condition and estimated as stirred text at a first step based on the plaintext and the estimated parameter A" is shown in '095 col. 6, lines 1-40;

"an encryption control part for using and allowing an encryption apparatus to calculate ciphertext based on the plaintext accepted by the estimated stirred text calculating part" is disclosed in '095 col. 6, line 64 through col. 7, line 10;

"a last-but-one-step estimated stirred text calculating part for accepting the ciphertext calculated under the control of the encryption control part, calculating a last-step estimated extended key estimated as an extended key at a last step by exhaustive search" is taught in '095 col. 5, line 40 through col. 6, line 40;

"and calculating last-but-one-step estimated stirred text estimated as stirred text at a last-but-one step based on the ciphertext and the last-step estimated extended key; is taught in '095 col. 6, lines 7-25;

"a key verification part for formulating an encryption equation with higher order differences based on the first-step estimated stirred text accepted by the estimated stirred text calculating part and the last-but-one-step estimated stirred text calculated by the last-but-one-step estimated stirred text calculating part" is taught in '095 col. 10, lines 39-67;

"processing it by an algebraic technique to try to calculate a last-but-one-step extended key estimated as an extended key at the last-but-one step" in '095 col. 11, lines 1-25;

the following is not explicitly taught in '095:

"verifying the parameter A and the last-step estimated extended key to be right by detecting that calculation is possible, and outputting a calculation impossible signal when detecting that calculation is impossible" however '948 teaches the maximum differential probability is an important measure for estimating the strength of a given function in col. 5, lines 32-60;

"and a decryption control part for accepting the calculation impossible signal, and controlling the estimated stirred text calculating part, the encryption control part, the last-but-one-step estimated stirred text calculation part and the key verification part to allow the last-but-one-step estimated extended key to be calculated" however '948 teaches decryption has a structure obtained by reversing the encryption apparatus (the same key is used) in col. 17, lines 27-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention a symmetric block cipher using multiples stages with modified type-I and type-3 Feistel networks taught in '095 to include a means to calculate the probability of the last-step extended key. One of ordinary skill in the art would have been motivated to perform such a modification because the typical Feistel type encryption scheme need to improve strength analysis see '948 (col. 1, lines 21 et seq,) "Typical fundamental structures of common key block encryption scheme include SPN type and Feistel type. For both structures, a design method for improving strength evaluation and resiliency against differential/linear cryptanalysis have been studied (reference [1] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers & E. Dcwin, "The Cipher SHARK," Fast Software Encryption, LNCS 1039, 1996, reference [2] Kazumaro Aoki, Kazuo Ota, "More Strict Evaluation of Maximum Mean Differential Probability and Maximum Mean Linear Probability," SCIS 96-4A, 1996, reference [3], Mitsuru Matsui, "Block encryption scheme MISTY," ISEC 96-11, 1996)".

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Shimoyama et al.	U.S. Patent Pub.No. 2002/0021801	issued dated: Feb. 21, 2002
Roeise	U.S. Patent No. 7,043,016	issued dated: May 09, 2006
Luyster	U.S. Patent No. 6,751,319	issued dated: Jun. 15, 2004

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
22 June 2007